THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
GREENBELT DIVISION

JANE DOE

and

JOHN DOE,

on behalf of themselves and all others similarly situated,

Plaintiffs,

vs.

US FERTILITY, LLC,

a Maryland limited liability company,

Defendant.

Case No.:

CLASS ACTION COMPLAINT

DEMAND FOR JURY TRIAL

Plaintiffs Jane Doe and John Doe ("Plaintiffs"), individually and on behalf of all others similarly situated, bring this Class Action Complaint against US Fertility, LLC (collectively, "US Fertility" or "Defendant"), and allege, upon personal knowledge as to their own actions and their counsels' investigations, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for its failure to properly secure and safeguard personal identifiable information and protected health information that Defendant acquired from or created for its patients. Defendant required this information from its patients or created this information for its patients as a condition or result of medical treatment, including without limitation, names, addresses, dates of birth, MPI (patient identification) numbers, Social Security numbers, driver's license / state ID numbers, passport numbers, credit/debit card information, and financial account information (collectively, "personal identifiable information" or "PII") as well as medical treatment/diagnosis information, medical record information, and

health insurance/claims information (collectively, "protected health information" or "PHI"). Plaintiffs also allege Defendant failed to provide timely, accurate, and adequate notice to Plaintiffs and similarly situated current and former patients (collectively, "Class Members") that their PII and PHI had been lost and precisely what types of information was unencrypted and in the possession of unknown third parties.

2. According to its website, Defendant is the largest network of fertility centers in the United States. Defendant provides information technology platforms and services to infertility clinics in numerous States, including Alabama, California, Florida, Georgia, Idaho, Illinois, Maryland, Missouri, Nevada, New York, North Carolina, Pennsylvania, Utah, Virginia, and Washington. In order to obtain medical treatment, Plaintiffs and other patients of Defendant entrust and provide to Defendant an extensive amount of PII. Defendant also creates PII and PHI for its patients. Defendant retains this information on computer hardware—even after the treatment relationship ends. Defendant asserts that it understands the importance of protecting information.

3. On or before September 20, 2020, Defendant determined that an unauthorized actor acquired a limited number of files during a period of unauthorized access, which occurred between August 12, 2020 and September 14, 2020 (the "Data Breach").

4. On or before November 13, 2020, Defendant learned that the files accessed and acquired during the Data Breach contained the PII of Defendant's current and former patients, including Plaintiffs and Class Members. Defendant subsequently confirmed that these files also included PHI of Defendant's current and former patients, including Plaintiffs and Class Members.

5. In a "Notice of Data Incident," dated January 8, 2021, Defendant advised that it was informing its current and former patients of the Data Breach.

6. By obtaining, collecting, using, and deriving a benefit from Plaintiffs' and Class Members' PII and PHI, Defendant assumed legal and equitable duties to those individuals. Defendant admits that the unencrypted PII and PHI exposed to "unauthorized activity" included names, addresses, dates of birth, MPI numbers, Social Security numbers, driver's license / state ID numbers, passport numbers, medical treatment/diagnosis information, medical record information, health insurance/claims information, credit/debit card information, and financial account information.

7. The exposed PII and PHI of Defendant's current and former patients can be sold on the dark web. Hackers can access and then offer for sale the unencrypted, unredacted PII to criminals. Defendant's current and former patients face a lifetime risk of identity theft, which is heightened here by the loss of Social Security numbers, driver's license / state ID numbers, and passport numbers.

8. This PII and PHI was compromised due to Defendant's negligent and/or careless acts and omissions and the failure to protect PII and PHI of Defendant's current and former patients. In addition to Defendant's failure to prevent the Data Breach, after discovering the breach, Defendant waited several months to report it to the states' Attorneys General and affected individuals.

9. As a result of this delayed response, Plaintiffs and Class Members had no idea their PII and PHI had been compromised, and that they were, and continue to be, at significant risk of identity theft and various other forms of personal, social, and financial harm. The risk will remain for their respective lifetimes.

10. Plaintiffs bring this action on behalf of all persons whose PII and/or PHI was compromised as a result of Defendant's failure to: (i) adequately protect the PII and PHI of

Defendant's current and former patients; (ii) warn Defendant's current and former patients of Defendant's inadequate information security practices; and (iii) effectively secure hardware containing protected PII and PHI using reasonable and effective security procedures free of vulnerabilities and incidents. Defendant's conduct amounts to negligence and violates federal and state statutes.

11. Plaintiffs and Class Members have suffered injury as a result of Defendant's conduct. These injuries include: (i) lost or diminished value of PII and PHI; (ii) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (iii) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach, including but not limited to lost time, and significantly (iv) the continued and certainly an increased risk to their PII and PHI, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) may remain backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI.

12. Defendant disregarded the rights of Plaintiffs and Class Members by intentionally, willfully, recklessly, or negligently failing to take and implement adequate and reasonable measures to ensure that Defendant's current and former patients' PII and PHI was safeguarded, failing to take available steps to prevent an unauthorized disclosure of data, and failing to follow applicable, required and appropriate protocols, policies and procedures regarding the encryption of data, even for internal use. As the result, the PII and PHI of Plaintiffs and Class Members was compromised through disclosure to an unknown and unauthorized third party. Plaintiffs and Class Members have a continuing interest in ensuring that their information is and remains safe, and they should be entitled to injunctive and other equitable relief.

II. PARTIES

13. Plaintiff Jane Doe is a Citizen of Florida residing in Hillsborough County, Florida. Ms. Doe received Defendant's *Notice of Data Incident*, dated January 8, 2021, on or about that date. Because of the nature of the medical services provided to Plaintiff, she is filing this complaint under Jane Doe.

14. Plaintiff John Doe is a Citizen of Pennsylvania residing in Montgomery County, Pennsylvania. Mr. Doe received Defendant's *Notice of Data Incident*, dated January 8, 2021, on or about that date. Because of the nature of the medical services provided to Plaintiff, he is filing this complaint under John Doe.

15. Defendant US Fertility, LLC. is a corporation organized under the laws of Delaware, headquartered at 9600 Blackwell Road, Suite 500, Rockville, MD, with its principal place of business in Rockville, MD.

16. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiffs. Plaintiffs will seek leave of court to amend this complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

17. All of Plaintiffs' claims stated herein are asserted against Defendant and any of their owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

18. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of $5 million, exclusive of interest and costs, there are more than 100 members in the

proposed class, and at least one other Class Member (including named Plaintiff Jane Doe, a Citizen of Florida) is a citizen of a state different from Defendant to establish minimal diversity.

19. The District of Maryland has personal jurisdiction over Defendant named in this action because Defendant is headquartered in this District and Defendant conducts substantial business in Maryland and this District.

20. Venue is proper in this District under 28 U.S.C. §1391(b) because Defendant is headquartered in this District and a substantial part of the events or omissions giving rise to Plaintiffs' claims occurred in this District.

IV. FACTUAL ALLEGATIONS

Background

21. Defendant is the largest network of fertility centers in the United States and provides information technology platforms and services to infertility clinics throughout the United States.

22. Plaintiffs and Class Members treated by Defendant were required to provide some of their most sensitive and confidential information, including names, addresses, dates of birth, Social Security numbers, driver's license / state ID numbers, passport numbers, health insurance information, credit/debit card information, and financial account information and other personal identifiable information. This information is static, does not change, and can be used to commit myriad financial crimes.

23. In providing treatment to Plaintiffs and Class Members, Defendant created additional sensitive personal information about Plaintiffs and Class Members, including MPI numbers, medical treatment/diagnosis information, medical record information, and health claims information.

24. Plaintiffs and Class Members, as current and former patients, relied on Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Defendant's current and former patients demand security to safeguard their PII and PHI.

25. Defendant had a duty to adopt reasonable measures to protect Plaintiffs' and Class Members' PII and PHI from involuntary disclosure to third parties.

The Data Breach

26. Beginning on or about January 8, 2021, Defendant sent its current and former patients a *Notice of Data Incident*.[1] Defendant informed the recipients of the notice that:

> We are writing to make you aware of a recent incident that may affect the privacy of some of your protected health information.
>
> **What Happened?** On September 14, 2020, USF experienced an IT security event (the "Incident") that involved the inaccessibility of certain computer systems on our network as a result of a malware infection. We responded to the Incident immediately and retained third-party computer forensic specialists to assist in our investigation. Through our immediate investigation and response, we determined that data on a number of servers and workstations connected to our domain had been encrypted by ransomware. We proactively removed a number of systems from our network upon discovering the Incident. With the assistance of our third-party computer forensic specialists, we remediated the malware identified, ensured the security of our environment, and reconnected systems on September 20, 2020. We also notified federal law enforcement authorities of the Incident and continue to cooperate with their investigation. The forensic investigation is now concluded and confirmed that the unauthorized actor acquired a limited number of files during the period of unauthorized access, which occurred between August 12, 2020 and September 14, 2020, when the ransomware was executed.
>
> **What Information Was Involved?** We have been working diligently with a specialized team of third-party data auditors to perform a comprehensive review of all information contained in the

[1] Ex. 1 (available at https://ago.vermont.gov/wp-content/uploads/2021/01/2021-01-08-US-Fertility-LLC-Notice-of-Data-Breach-to-Consumers.pdf) (last visited Jan. 28, 2021).

> files accessed without authorization as a result of the Incident. The purpose of this review was to accurately identify any individuals whose personal information may have been present within the impacted files and therefore accessible to the unauthorized actor. We recently received the results of this review and determined on December 4, 2020 that the following information relating to you was included in the impacted files when they were accessed without authorization: name and <<Breached Elements>>. The impacted files may have also contained your date of birth. Please note, however, that we have no evidence of actual misuse of your information as a result of the Incident.[2]

27. On or about January 8, 2021, Defendant sent data breach notifications to various state Attorneys General, including Vermont's Attorney General TJ Donovan, signed by Carrie Roll, Defendant's General Counsel.[3]

28. Defendant admitted in the *Notice of Data Incident* and the letters to the Attorneys General that unauthorized third persons accessed files that contained sensitive information about current and former patients of Defendant, including names, addresses, dates of birth, MPI (patient identification) numbers, and/or Social Security numbers.

29. In response to the Data Breach, Defendant claims that it

> has taken the following actions to mitigate any risk of compromise to your information and to better prevent a similar event from recurring: (1) fortified the security of our firewall; (2) utilized the forensic specialists engaged to monitor network activity and remediate any suspicious activity; (3) provided notification to potentially impacted individuals as quickly as possible. We are also adapting our existing employee training protocols relating to data protection and security, including training targeted at recognizing phishing emails. We believe these steps will be effective in mitigating any potential harm to you. As always, we encourage you to review your account statements, explanations of benefits, and credit reports carefully for unexpected activity and to report any questionable activity to the associated institutions immediately. immediately launched an investigation, we engaged an independent computer forensics firm to determine what happened and whether personal information had been accesses or acquired without

[2] Ex. 1, p.1.
[3] *Id.*

> authorization…. We have also implemented additional safeguards to help ensure the security of our email environment and to reduce the risk of a similar incident occurring in the future.[4]

30. In January 2021, Defendant posted an amended *Notice of Data Security Incident* on its website stating that, in addition to the information previously identified as exposed, the Data Breach also resulted in the exposure of PHI and other PII, including "driver's license / state ID numbers, passport numbers, medical treatment/diagnosis information, medical record information, health insurance/claims information, credit/debit card information, and financial account information."[5] These items were not mentioned in the notice previously sent to Defendant's current and former patients or in the notice previously published on Defendant's website.[6]

31. Plaintiffs' and Class Members' unencrypted information may end up for sale on the dark web, or simply fall into the hands of companies that will use the detailed PII and PHI for targeted marketing without the approval of the affected current and former patients. Unauthorized individuals can easily access the PII and PHI of Defendant's current and former patients.

32. Defendant did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information they were maintaining for current and former patients, causing Plaintiffs' and Class Members' PII and PHI to be exposed.

Defendant Acquires, Collects, Creates, and Stores Plaintiffs' and Class Members' PII and PHI.

33. Defendant acquired, collected, created, and stored Defendant's current and former patients' PII and PHI.

34. As a condition of maintaining treatment with Defendant, Defendant requires that

---

[4] *Id.*

[5] Ex. 2 (available at https://www.usfertility.com/wp-content/uploads/2021/01/USF-Notice-Security.pdf) (last visited Jan. 28, 2021).

[6] Ex. 3 (available at https://www.usfertility.com/wp-content/uploads/2020/11/Version-4142340_2-Website-Notice-11.25.2020_Final.pdf) (last visited Jan. 28, 2021).

its patients entrust Defendant with highly confidential PII.

35. By obtaining, collecting, creating, and storing Plaintiffs' and Class Members' PII and PHI, Defendant assumed legal and equitable duties and knew or should have known that they were responsible for protecting Plaintiffs' and Class Members' PII and PHI from disclosure.

36. Plaintiffs and the Class Members have taken reasonable steps to maintain the confidentiality of their PII and PHI. Plaintiffs and the Class Members, as current and former patients, relied on the Defendant to keep their PII and PHI confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

Securing PII and PHI and Preventing Breaches

37. Defendant could have prevented this Data Breach by properly securing and encrypting Plaintiffs' and Class Members' PII and PHI. Or Defendant could have destroyed the data, especially old data from former patients that Defendant had no legal duty to retain.

38. Defendant's negligence in safeguarding Defendant's current and former patients' PII and PHI is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

39. Despite the prevalence of public announcements of data breach and data security compromises, Defendant failed to take appropriate steps to protect the PII and PHI of Plaintiffs and the proposed Class from being compromised.

40. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[7] The FTC describes "identifying information" as "any name or number that may be used, alone or

[7] 17 C.F.R. § 248.201 (2013).

in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[8]

41. The ramifications of Defendant's failure to keep secure Defendant's current and former patients' PII and PHI are long lasting and severe. Once PII and PHI is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Value of Personal Identifiable Information

42. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from $40 to $200, and bank details have a price range of $50 to $200.[9] Experian reports that a stolen credit or debit card number can sell for $5 to $110 on the dark web.[10] Criminals can also purchase access to entire company data breaches from $900 to $4,500.[11]

43. Social Security numbers, for example, are among the worst kind of personal information to have stolen because they may be put to a variety of fraudulent uses and are difficult for an individual to change. The Social Security Administration stresses that the loss of an

---

[8] *Id.*

[9] *Your personal data is for sale on the dark web. Here's how much it costs,* Digital Trends, Oct. 16, 2019, *available at*: https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/ (last accessed Jan. 26, 2021).

[10] *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, *available at*: https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/ (last accessed Jan. 26, 2021).

[11] *In the Dark*, VPNOverview, 2019, *available at*: https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/ (last accessed Jan. 26, 2021).

individual's Social Security number, as is the case here, can lead to identity theft and extensive financial fraud:

> A dishonest person who has your Social Security number can use it to get other personal information about you. Identity thieves can use your number and your good credit to apply for more credit in your name. Then, they use the credit cards and don't pay the bills, it damages your credit. You may not find out that someone is using your number until you're turned down for credit, or you begin to get calls from unknown creditors demanding payment for items you never bought. Someone illegally using your Social Security number and assuming your identity can cause a lot of problems.[12]

44. What is more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

45. Even then, a new Social Security number may not be effective. According to Julie Ferguson of the Identity Theft Resource Center, "The credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[13]

46. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach, because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to

[12] Social Security Administration, *Identity Theft and Your Social Security Number*, *available at*: https://www.ssa.gov/pubs/EN-05-10064.pdf (last accessed Jan. 26, 2021).
[13] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), *available at*: http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft (last accessed Jan. 26, 2021).

change—name, address, date of birth, and Social Security number.

47. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information, personally identifiable information and Social Security numbers are worth more than 10x on the black market."[14]

48. Among other forms of fraud, identity thieves may obtain driver's licenses, government benefits, medical services, and housing or even give false information to police.

49. The PII of Plaintiffs and Class Members was taken by hackers to engage in identity theft or and or to sell it to others criminals who will purchase the PII for that purpose. The fraudulent activity resulting from the Data Breach may not come to light for years..

50. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office ("GAO"), which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[15]

51. At all relevant times, Defendant knew, or reasonably should have known, of the importance of safeguarding Defendant's current and former patients' PII, including Social Security numbers and dates of birth, and of the foreseeable consequences that would occur if Defendant's

[14] Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), *available at*: https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Jan. 26, 2021).
[15] *Report to Congressional Requesters*, GAO, at 29 (June 2007), *available at:* http://www.gao.gov/new.items/d07737.pdf (last accessed Jan. 26, 2021).

data security system was breached, including, specifically, the significant costs that would be imposed on Defendant's current and former patients as a result of a breach.

52. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

53. Defendant was, or should have been, fully aware of the unique type and the significant volume of data on Defendant's network, amounting to potentially thousands or tens or hundreds of thousands of individuals' detailed, personal information and thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

54. To date, Defendant has offered their current and former patients only one year of credit monitoring and identity restoration services through a single provider, TransUnion. The offered service is inadequate to protect Plaintiffs and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

55. The injuries to Plaintiffs and Class Members were directly and proximately caused by Defendant's failure to implement or maintain adequate data security measures for the PII of Defendant's current and former patients.

Plaintiff Jane Doe's Experience

56. In or around 2009, Plaintiff Jane Doe was a patient of Defendant. As a condition for treatment, she was required to provide her PII, including but not limited to her name, address, date of birth, and Social Security number.

57. Ms. Doe received the Notice of Data Incident, dated January 8, 2021, on or about that date. The notice did not reveal that Ms. Doe's PHI had been exposed.

58. As a result of the Notice of Data Incident, Ms. Doe spent time dealing with the

consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Incident, exploring credit monitoring and identity theft insurance options, signing up and routinely monitoring the credit monitoring offered by Defendant, and self-monitoring her accounts. This time has been lost forever and cannot be recaptured.

59. Additionally, Ms. Doe is very careful about sharing her PII. She has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

60. Ms. Doe stores any documents containing her PII or PHI in a safe and secure location or destroys the documents. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

61. Ms. Doe suffered actual injury in the form of damages to and diminution in the value of her PII—a form of intangible property that Ms. Doe entrusted to Defendant for the purpose of her treatment, which was compromised in and as a result of the Data Breach.

62. Ms. Doe suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of her privacy.

63. Ms. Doe has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII and PHI, especially her Social Security number, in combination with her name and date of birth, being placed in the hands of unauthorized third-parties and possibly criminals.

64. Ms. Doe has a continuing interest in ensuring that her PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

Plaintiff John Doe's Experience

65. In or around 2019, Plaintiff John Doe was a patient of Defendant. As a condition

for treatment, he was required to provide his PII, including but not limited to his name, address, date of birth, and Social Security number.

66. Mr. Doe received the Notice of Data Incident, dated January 8, 2021, on or about that date. The notice did not reveal that Mr. Doe's PHI had been exposed.

67. As a result of the Notice of Data Incident, Mr. Doe spent time dealing with the consequences of the Data Breach, which includes time spent verifying the legitimacy of the Notice of Data Incident, exploring credit monitoring and identity theft insurance options, signing up and routinely monitoring the credit monitoring offered by Defendant, and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

68. Additionally, Mr. Doe is very careful about sharing his PII. He has never knowingly transmitted unencrypted PII over the internet or any other unsecured source.

69. Mr. Doe stores any documents containing his PII or PHI in a safe and secure location or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

70. Mr. Doe suffered actual injury in the form of damages to and diminution in the value of his PII—a form of intangible property that Mr. Doe entrusted to Defendant for the purpose of his treatment, which was compromised in and as a result of the Data Breach.

71. Mr. Doe suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and has anxiety and increased concerns for the loss of his privacy.

72. Mr. Doe has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from his PII and PHI, especially his Social Security number, in combination with his name and date of birth, being placed in the hands of unauthorized third-parties and possibly criminals.

73. Mr. Doe has a continuing interest in ensuring that his PII and PHI, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

V. CLASS ALLEGATIONS

74. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

75. The Nationwide Class that Plaintiffs seek to represent is defined as follows:

> All individuals whose PII and/or PHI was compromised in the data breach first announced by Defendant on or about January 8, 2021 (the "Nationwide Class").

76. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff Jane Doe asserts claims on behalf of a separate statewide subclass, defined as follows:

> All individuals who are residents of Florida and whose PII and/or PHI was compromised in the data breach first announced by Defendant on or about January 8, 2021 (the "Florida Class").

77. Pursuant to Rule 23, and in the alternative to claims asserted on behalf of the Nationwide Class, Plaintiff John Doe asserts claims on behalf of a separate statewide subclass, defined as follows:

> All individuals who are residents of Pennsylvania and whose PII and/or PHI was compromised in the data breach first announced by Defendant on or about January 8, 2021 (the "Pennsylvania Class").

78. Excluded from the Classes are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant has a controlling interest; all individuals who make a timely election to be excluded

from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards, sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

79. Plaintiffs reserve the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

80. Numerosity, Fed R. Civ. P. 23(a)(1): The Nationwide Class (the "Class") are so numerous that joinder of all members is impracticable. Defendant has identified thousands of current and former patients whose PII and PHI may have been improperly accessed in the Data Breach, and the Class is apparently identifiable within Defendant's records.

81. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

a. Whether and to what extent Defendant had a duty to protect the PII and PHI of Plaintiffs and Class Members;

b. Whether Defendant had respective duties not to disclose the PII and PHI of Plaintiffs and Class Members to unauthorized third parties;

c. Whether Defendant had a duty not to use the PII and PHI of Plaintiffs and Class Members for non-business purposes;

d. Whether Defendant failed to adequately safeguard the PII and PHI of Plaintiffs and Class Members;

e. Whether and when Defendant actually learned of the Data Breach;

f. Whether Defendant adequately, promptly, and accurately informed Plaintiffs and

Class Members that their PII and PHI had been compromised;

g. Whether Defendant violated the law by failing to promptly notify Plaintiffs and Class Members that their PII and PHI had been compromised;

h. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

i. Whether Defendant adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;

j. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class Members;

k. Whether Plaintiffs and Class Members are entitled to actual, damages, and/or statutory damages as a result of Defendant's wrongful conduct;

l. Whether Plaintiffs and Class Members are entitled to restitution as a result of Defendant's wrongful conduct; and

m. Whether Plaintiffs and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

82. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiffs' claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendant's misfeasance.

83. Policies Generally Applicable to the Class: This class action is also appropriate for certification because Defendant has acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class Members and making final injunctive relief appropriate with respect

to the Class as a whole. Defendant's policies challenged herein apply to and affect Class Members uniformly and Plaintiffs' challenge of these policies hinges on Defendant's conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiffs.

84. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiffs will fairly and adequately represent and protect the interests of the Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Members of the Class. Plaintiffs seek no relief that is antagonistic or adverse to the Members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiffs have retained counsel experienced in complex class action litigation, and Plaintiffs intend to prosecute this action vigorously.

85. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendant. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

86. The nature of this action and the nature of laws available to Plaintiffs and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiffs and Class Members for the wrongs alleged because Defendant would

necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

87. The litigation of the claims brought herein is manageable. Defendant's uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

88. Adequate notice can be given to Class Members directly using information maintained in Defendant's records.

89. Unless a Class-wide injunction is issued, Defendant may continue in its failure to properly secure the PII and PHI of Class Members, Defendant may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendant may continue to act unlawfully as set forth in this Amended Complaint.

90. Further, Defendant has acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

91. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would

advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Defendant owed a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

b. Whether Defendant breached a legal duty to Plaintiffs and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII and PHI;

c. Whether Defendant failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;

d. Whether an implied contract existed between Defendant on the one hand, and Plaintiffs and Class Members on the other, and the terms of that implied contract;

e. Whether Defendant breached the implied contract;

f. Whether Defendant adequately, and accurately informed Plaintiffs and Class Members that their PII and PHI had been compromised;

g. Whether Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;

h. Whether Defendant engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII and PHI of Plaintiffs and Class Members; and,

i. Whether Class Members are entitled to actual damages, statutory damages, injunctive relief, and/or punitive damages as a result of Defendant's wrongful conduct.

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

92. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 91.

93. As a condition of their treatment by Defendant, Defendant's current and former patients were obligated to provide Defendant with certain PII and PHI, including their names, addresses, dates of birth, Social Security numbers, driver's license / state ID numbers, passport numbers, credit/debit card information, financial account information, and health insurance information.

94. As a condition of their treatment by Defendant, Defendant created PII and PHI for Defendant's current and former patients, including their MPI numbers, medical treatment/diagnosis information, medical record information, and health claims information.

95. Plaintiffs and the Class Members entrusted their PII and PHI to Defendant on the premise and with the understanding that Defendant would safeguard their information, use their PII and PHI for business purposes only, and/or not disclose their PII and PHI to unauthorized third parties.

96. Defendant has full knowledge of the sensitivity of the PII and PHI and the types of harm that Plaintiffs and Class Members could and would suffer if the PII and PHI were wrongfully disclosed.

97. Defendant knew or reasonably should have known that the failure to exercise due

care in the collecting, storing, and using of its current and former patients' PII and PHI involved an unreasonable risk of harm to Plaintiffs and Class Members, even if the harm occurred through the criminal acts of a third party.

98. Defendant had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendant's security protocols to ensure that Plaintiffs' and Class Members' information in Defendant's possession was adequately secured and protected.

99. Defendant also had a duty to exercise appropriate clearinghouse practices to remove former patients' PII it was no longer required to retain pursuant to regulations.

100. Defendant also had a duty to have procedures in place to detect and prevent the improper access and misuse of Plaintiffs' and Class Members' PII and PHI.

101. Defendant's duty to use reasonable security measures arose as a result of the special relationship that existed between Defendant and Plaintiffs and Class Members. That special relationship arose because Plaintiffs and Class Members entrusted Defendant with their confidential PII and PHI, a necessary part of obtaining treatment from Defendant.

102. Defendant was subject to an "independent duty," untethered to any contract between Defendant and Plaintiffs or Class Members.

103. A breach of security, unauthorized access, and resulting injury to Plaintiffs and the Class Members was reasonably foreseeable, particularly in light of Defendant's inadequate security practices.

104. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendant knew or should have known of the

inherent risks in collecting and storing the PII and PHI of Plaintiffs and the Class, the critical importance of providing adequate security of that PII and PHI, and the necessity for encrypting PII and PHI stored on Defendant's systems.

105. Defendant's own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendant's misconduct included, but was not limited to, its failure to take the steps and opportunities to prevent the Data Breach as set forth herein. Defendant's misconduct also included its decision not to comply with industry standards for the safekeeping of Plaintiffs' and Class Members' PII, including basic encryption techniques freely available to Defendant.

106. Plaintiffs and Class Members had no ability to protect their PII and PHI that was in, and possibly remains in, Defendant's possession.

107. Defendant was in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

108. Defendant had and continues to have a duty to adequately disclose that the PII and PHI of Plaintiffs and Class Members within Defendant's possession might have been compromised, how it was compromised, and precisely the types of data that were compromised and when. Such notice was necessary to allow Plaintiffs and the Class Members to take steps to prevent, mitigate, and repair any identity theft and the fraudulent use of their PII and PHI by third parties.

109. Defendant had a duty to employ proper procedures to prevent the unauthorized dissemination of the PII and/or PHI of Plaintiffs and Class Members.

110. Defendant has admitted that the PII and PHI of Plaintiffs and Class Members was wrongfully lost and disclosed to unauthorized third persons as a result of the Data Breach.

111. Defendant, through its actions and/or omissions, unlawfully breached its duties to

Plaintiffs and Class Members by failing to implement industry protocols and exercise reasonable care in protecting and safeguarding the PII and PHI of Plaintiffs and Class Members during the time the PII and PHI was within Defendant's possession or control.

112. Defendant improperly and inadequately safeguarded the PII and PHI of Plaintiffs and Class Members in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

113. Defendant failed to heed industry warnings and alerts to provide adequate safeguards to protect its current and former patients' PII and PHI in the face of increased risk of theft.

114. Defendant, through its actions and/or omissions, unlawfully breached its duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of its current and former patients' PII and PHI.

115. Defendant breached its duty to exercise appropriate clearinghouse practices by failing to remove former patients' PII and PHI it was no longer required to retain pursuant to regulations.

116. Defendant, through its actions and/or omissions, unlawfully breached its duty to adequately and timely disclose to Plaintiffs and Class Members the existence and scope of the Data Breach.

117. But for Defendant's wrongful and negligent breach of duties owed to Plaintiffs and Class Members, the PII and PHI of Plaintiffs and Class Members would not have been compromised.

118. There is a close causal connection between Defendant's failure to implement security measures to protect the PII and PHI of Plaintiffs and Class Members and the harm suffered

or risk of imminent harm suffered by Plaintiffs and the Class. Plaintiffs' and Class Members' PII and PHI was lost and accessed as the proximate result of Defendant's failure to exercise reasonable care in safeguarding such PII and PHI by adopting, implementing, and maintaining appropriate security measures.

119. Additionally, Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII and PHI. The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

120. Defendant violated Section 5 of the FTC Act by failing to use reasonable measures to protect PII and PHI and not complying with applicable industry standards, as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII and PHI it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and Class Members.

121. Defendant's violation of Section 5 of the FTC Act constitutes negligence *per se*.

122. Plaintiffs and Class Members are within the class of persons that the FTC Act was intended to protect.

123. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and the Class.

124. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i)

actual identity theft; (ii) the loss of the opportunity of how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the current and former patients' PII and PHI in its continued possession; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

125. As a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

126. Additionally, as a direct and proximate result of Defendant's negligence and negligence *per se*, Plaintiffs and Class members have suffered and will suffer the continued risks of exposure of their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI in their continued possession.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiffs and the Nationwide Class)

127. Plaintiffs and Class Members re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 91.

128. Defendant required Plaintiffs and Class Members to provide their personal information, including names, addresses, dates of birth, Social Security numbers, driver's license / state ID numbers, passport numbers, credit/debit card information, financial account information, health insurance information, and other personal information as a condition of their treatment.

129. As a condition of Plaintiffs' and Class Members' treatment with Defendant, they provided their personal information to Defendant and Defendant created additional information about Plaintiffs, including MPI numbers, medical treatment/diagnosis information, medical record information, and health claims information. In so doing, Plaintiffs and Class Members entered into implied contracts with Defendant by which Defendant agreed to safeguard and protect such information, to keep such information secure and confidential, and to timely and accurately notify Plaintiffs and Class Members if their data had been breached, compromised, or stolen.

130. Plaintiffs and Class Members fully performed their obligations under the implied contracts with Defendant.

131. Defendant breached the implied contracts it made with Plaintiffs and Class Members by failing to safeguard and protect their personal information and by failing to provide timely and accurate notice to them that personal was compromised as a result of the data breach.

132. As a direct and proximate result of Defendant's above-described breach of implied contract, Plaintiffs and Class Members have suffered (and will continue to suffer) ongoing, imminent, and impending threat of identity theft crimes, fraud, and abuse, resulting in monetary

loss and economic harm; actual identity theft crimes, fraud, and abuse, resulting in monetary loss and economic harm; loss of the confidentiality of the stolen confidential data; the illegal sale of the compromised data on the dark web; expenses and/or time spent on credit monitoring and identity theft insurance; time spent scrutinizing bank statements, credit card statements, and credit reports; expenses and/or time spent initiating fraud alerts, decreased credit scores and ratings; lost work time; and other economic and non-economic harm.

COUNT III
Invasion of Privacy
(On Behalf of Plaintiffs and the Nationwide Class)

133. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 91.

134. Plaintiffs and Class Members had a legitimate expectation of privacy to their PII and PHI and were entitled to the protection of this information against disclosure to unauthorized third parties.

135. Defendant owed a duty to its current and former patients, including Plaintiffs and Class Members, to keep their PII and PHI contained as a part thereof, confidential.

136. Defendant failed to protect and released to unknown and unauthorized third parties the PII and/or PHI of Plaintiffs and Class Members.

137. Defendant allowed unauthorized and unknown third parties access to and examination of the PII and/or PHI of Plaintiffs and Class Members, by way of Defendant's failure to protect the PII and PHI.

138. The unauthorized release to, custody of, and examination by unauthorized third parties of the PII and/or PHI of Plaintiffs and Class Members is highly offensive to a reasonable person.

139. The intrusion was into a place or thing, which was private and is entitled to be private. Plaintiffs and Class Members disclosed their PII and PHI to Defendant, or allowed Defendant to create their PII and PHI, as part of their treatment by Defendant, but privately with an intention that the PII and PHI would be kept confidential and would be protected from unauthorized disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

140. The Data Breach at the hands of Defendant constitutes an intentional interference with Plaintiffs and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

141. Defendant acted with a knowing state of mind when its permitted the Data Breach to occur because it was with actual knowledge that its information security practices were inadequate and insufficient.

142. Because Defendant acted with this knowing state of mind, it had notice and knew the inadequate and insufficient information security practices would cause injury and harm to Plaintiffs and Class Members.

143. As a proximate result of the above acts and omissions of Defendant, the PII and PHI of Plaintiffs and Class Members was disclosed to third parties without authorization, causing Plaintiffs and Class Members to suffer damages.

144. Unless and until enjoined, and restrained by order of this Court, Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the PII and PHI maintained by Defendant can be viewed, distributed, and used by unauthorized persons for years to come. Plaintiffs and Class Members have no adequate remedy

at law for the injuries in that a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and the Class.

COUNT IV
Breach of Confidence
(On Behalf of Plaintiffs and the Nationwide Class)

145. Plaintiffs re-allege and incorporate by reference herein all of the allegations contained in paragraphs 1 through 91.

146. At all times during Plaintiffs' and Class Members' interactions with Defendant, Defendant was fully aware of the confidential and sensitive nature of Plaintiffs' and Class Members' PII and PHI that Plaintiffs and Class Members treated by Defendant provided to Defendant or allowed Defendant to create.

147. As alleged herein and above, Defendant's relationship with Plaintiffs and Class Members was governed by terms and expectations that Plaintiffs' and Class Members' PII and PHI would be collected, stored, and protected in confidence, and would not be disclosed to unauthorized third parties.

148. Plaintiffs and Class Members treated by Defendant provided Plaintiffs' and Class Members' PII and PHI to Defendant with the explicit and implicit understandings that Defendant would protect and not permit the PII and/or PHI to be disseminated to any unauthorized third parties.

149. Plaintiffs and Class Members treated by Defendant also provided Plaintiffs' and Class Members' PII and PHI to Defendant with the explicit and implicit understandings that Defendant would take precautions to protect that PII from unauthorized disclosure.

150. Defendant voluntarily received in confidence Plaintiffs' and Class Members' PII and PHI with the understanding that PII and PHI would not be disclosed or disseminated to the public or any unauthorized third parties.

151. Due to Defendant's failure to prevent and avoid the Data Breach from occurring, Plaintiffs' and Class Members' PII and PHI was disclosed and misappropriated to unauthorized third parties beyond Plaintiffs' and Class Members' confidence, and without their express permission.

152. As a direct and proximate cause of Defendant's actions and/or omissions, Plaintiffs and Class Members have suffered damages.

153. But for Defendant's disclosure of Plaintiffs' and Class Members' PII and PHI in violation of the parties' understanding of confidence, their PII and PHI would not have been compromised, stolen, viewed, accessed, and used by unauthorized third parties. Defendant's Data Breach was the direct and legal cause of the theft of Plaintiffs' and Class Members' PII and/or PHI as well as the resulting damages.

154. The injury and harm Plaintiffs and Class Members suffered was the reasonably foreseeable result of Defendant's unauthorized disclosure of Plaintiffs' and Class Members' PII and/or PHI. Defendant knew or should have known its methods of accepting and securing Plaintiffs' and Class Members' PII was inadequate as it relates to, at the very least, securing servers and other equipment containing Plaintiffs' and Class Members' PII and PHI.

155. As a direct and proximate result of Defendant's breach of their confidence with Plaintiffs and Class Members, Plaintiffs and Class Members have suffered and will suffer injury, including but not limited to: (i) actual identity theft; (ii) the loss of the opportunity how their PII and PHI is used; (iii) the compromise, publication, and/or theft of their PII and PHI; (iv) out-of-

pocket expenses associated with the prevention, detection, and recovery from identity theft, tax fraud, and/or unauthorized use of their PII and PHI; (v) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from tax fraud and identity theft; (vi) costs associated with placing freezes on credit reports; (vii) the continued risk to their PII and PHI, which remain in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII and PHI of current and former patients; and (viii) future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the PII and PHI compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

156. As a direct and proximate result of Defendant's breaches of confidence, Plaintiffs and Class Members have suffered and will continue to suffer other forms of injury and/or harm, including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

COUNT V
Violation of the Florida Deceptive and Unfair Trade Practices Act,
(Fla. Stat. §§ 502.201, *et seq.*)
(On Behalf of Plaintiff Jane Doe and the Florida Class)

157. Plaintiff Jane Doe re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 91.

158. Defendant engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, Defendant obtained Plaintiff Jane Doe's and Florida Class members' PII and PHI through advertising, soliciting, providing, offering, and/or

distributing goods and services to Jane Doe and Florida Class members and the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

159. As alleged herein this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

a. failure to implement adequate data security practices to safeguard PII and PHI;

b. failure to make only authorized disclosures of current and former patients' PII and PHI;

c. failure to timely and accurately disclose the Data Breach to Plaintiff Jane Doe and Florida Class members;

d. failure to disclose that its computer systems and data security practices were inadequate to safeguard PII and PHI from theft; and

e. failure to timely and accurately disclose the Data Breach to Plaintiff Jane Doe and Florida Class members.

160. Defendant's actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendant engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to its current and former patients.

161. In committing the acts alleged above, Defendant engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to its current and former patients that it did not follow industry best practices for the collection, use, and storage of PII and PHI.

162. As a direct and proximate result of Defendant's conduct, Plaintiff Jane Doe and Florida Class members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with

procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

163. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff Jane Doe and Florida Class members have been damaged and are entitled to recover actual damages, an order providing declaratory and injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

164. Also as a direct result of Defendant's knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiff Jane Doe and Florida Class members are entitled to damages as well as injunctive relief, including, but not limited to:

f. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

g. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

h. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

i. Ordering that Defendant segment PII and PHI by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant's systems;

j. Ordering that Defendant purge, delete, and destroy in a reasonable secure manner PII not necessary for its provisions of services;

k. Ordering that Defendant conduct regular database scanning and securing checks;

l. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

m. Ordering Defendant to meaningfully educate its current and former patients about the threats they face as a result of the loss of their PII and PHI to third parties, as well as the steps Defendant's current and former patients must take to protect themselves.

COUNT VI
Violation of the Pennsylvania Unfair Trade Practices and Consumer Protection Law, (73 P.S. §§ 202-1, *et seq.*)
(On Behalf of Plaintiff John Doe and the Pennsylvania Class)

165. Plaintiff John Doe re-alleges and incorporates by reference herein all of the allegations contained in paragraphs 1 through 91.

166. Defendant engaged in the conduct alleged in this Complaint through transactions in and involving trade and commerce. Mainly, Defendant obtained Plaintiff John Doe's and Pennsylvania Class members' PII and PHI through trade or commerce directly or indirectly affecting Plaintiff John Doe and Pennsylvania Class members and the Data Breach occurred through the use of the internet, an instrumentality of interstate commerce.

167. As alleged herein this Complaint, Defendant engaged in unfair or deceptive acts or practices in the conduct of consumer transactions, including, among other things, the following:

n. failure to implement adequate data security practices to safeguard PII and PHI;

o. failure to make only authorized disclosures of current and former patients' PII and PHI;

p. failure to timely and accurately disclose the Data Breach to Plaintiff John Doe and Pennsylvania Class members;

q. failure to disclose that its computer systems and data security practices were inadequate to safeguard PII and PHI from theft; and

r. failure to timely and accurately disclose the Data Breach to Plaintiff John Doe and Pennsylvania Class members.

168. Defendant's actions constitute unconscionable, deceptive, or unfair acts or practices because, as alleged herein, Defendant engaged in immoral, unethical, oppressive, and unscrupulous activities that are and were substantially injurious to its current and former patients.

169. In committing the acts alleged above, Defendant engaged in unconscionable, deceptive, and unfair acts and practices acts by omitting, failing to disclose, or inadequately disclosing to its current and former patients that it did not follow industry best practices for the collection, use, and storage of PII and PHI.

170. As a direct and proximate result of Defendant's conduct, Plaintiff John Doe and Pennsylvania Class members have been harmed and have suffered damages including, but not limited to: damages arising from identity theft and fraud; out-of-pocket expenses associated with procuring identity protection and restoration services; increased risk of future identity theft and fraud, and the costs associated therewith; and time spent monitoring, addressing and correcting the current and future consequences of the Data Breach.

171. As a direct and proximate result of the unconscionable, unfair, and deceptive acts or practices alleged herein, Plaintiff John Doe and Pennsylvania Class members have been

damaged and are entitled to recover actual damages, an order providing declaratory and injunctive relief, and reasonable attorneys' fees and costs, to the extent permitted by law.

172. Also as a direct result of Defendant's knowing violation of the Florida Unfair and Deceptive Trade Practices Act, Plaintiff John Doe and Pennsylvania Class members are entitled to damages as well as injunctive relief, including, but not limited to:

s. Ordering that Defendant engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

t. Ordering that Defendant engage third-party security auditors and internal personnel to run automated security monitoring;

u. Ordering that Defendant audit, test, and train its security personnel regarding any new or modified procedures;

v. Ordering that Defendant segment PII and PHI by, among other things, creating firewalls and access controls so that if one area of Defendant is compromised, hackers cannot gain access to other portions of Defendant's systems;

w. Ordering that Defendant purge, delete, and destroy in a reasonable secure manner PII and PHI not necessary for its provisions of services;

x. Ordering that Defendant conduct regular database scanning and securing checks;

y. Ordering that Defendant routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach; and

z. Ordering Defendant to meaningfully educate its current and former patients about the threats they face as a result of the loss of their PII and PHI to third parties, as well as the steps Defendant's current and former patients must take to protect themselves.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, on behalf of themselves and all Class Members, request judgment against Defendant and that the Court grant the following:

A. For an Order certifying the Nationwide Class, the Florida Class, and the Pennsylvania Class as defined herein, and appointing Plaintiffs and their Counsel to represent the Class;

B. For equitable relief enjoining Defendant from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiffs' and the Class Members' PII and PHI, and from refusing to issue prompt, complete, and accurate disclosures to Plaintiffs and the Class Members;

C. For injunctive relief requested by Plaintiffs, including but not limited to, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class Members, including but not limited to an order:

i. prohibiting Defendant from engaging in the wrongful and unlawful acts described herein;

ii. requiring Defendant to protect, including through encryption, all data collected through the course of its business in accordance with all applicable regulations, industry standards, and federal, state or local laws;

iii. requiring Defendant to delete, destroy, and purge the personal identifying information of Plaintiffs and Class Members unless Defendant can provide to the Court reasonable justification for the retention and use of such information when weighed against the privacy interests of Plaintiffs and Class Members;

iv. requiring Defendant to implement and maintain a comprehensive Information Security Program designed to protect the confidentiality and integrity of the personal identifying information of Plaintiffs and Class Members' personal identifying information;

v. prohibiting Defendant from maintaining Plaintiffs' and Class Members' personal identifying information on a cloud-based database;

vi. requiring Defendant to engage independent third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendant's systems on a periodic basis, and ordering Defendant to promptly correct any problems or issues detected by such third-party security auditors;

vii. requiring Defendant to engage independent third-party security auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train its security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiffs and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach;

xiii. requiring Defendant to implement a system of tests to assess its respective employees' knowledge of the education programs discussed in the preceding subparagraphs, as well as randomly and periodically testing employees compliance with Defendant's policies, programs, and systems for protecting personal identifying information;

xiv. requiring Defendant to implement, maintain, regularly review, and revise as necessary a threat management program designed to appropriately monitor Defendant's information networks for threats, both internal and external, and assess whether monitoring tools are appropriately configured, tested, and updated;

xv. requiring Defendant to meaningfully educate all Class Members about the threats that they face as a result of the loss of their confidential personal identifying information to third parties, as well as the steps affected individuals

must take to protect themselves;

xvi. requiring Defendant to implement logging and monitoring programs sufficient to track traffic to and from Defendant's servers; and for a period of 10 years, appointing a qualified and independent third party assessor to conduct a SOC 2 Type 2 attestation on an annual basis to evaluate Defendant's compliance with the terms of the Court's final judgment, to provide such report to the Court and to counsel for the class, and to report any deficiencies with compliance of the Court's final judgment; For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

D. For an award of damages, including actual, nominal, and consequential damages, as allowed by law in an amount to be determined;

E. For an award of attorneys' fees, costs, and litigation expenses, as allowed by law;

F. For prejudgment interest on all amounts awarded; and

G. Such other and further relief as this Court may deem just and proper.

DEMAND FOR JURY TRIAL

Plaintiffs hereby demand that this matter be tried before a jury.

Date: January 28, 2021

Respectfully Submitted,

/s/ George G. Triantis
GEORGE G. TRIANTIS, ESQ.
Bar No.: 21254
MORGAN & MORGAN, P.A.
201 N. Franklin Street, Suite 700
Tampa, Florida 33602
Telephone: 813-223-5505
Facsimile: 813-257-0572
Email: GTriantis@forthepeople.com

JOHN A. YANCHUNIS
(*Pro Hac Vice application forthcoming*)
RYAN D. MAXEY
(*Pro Hac Vice application forthcoming*)

MORGAN & MORGAN
201 N. Franklin Street, 7th Floor
Tampa, Florida 33602
(813) 223-5505
jyanchunis@ForThePeople.com
rmaxey@ForThePeople.com

RHINE LAW FIRM, P.C.
Joel R. Rhine
North Carolina State Bar No. 16028
Email: jrr@rhinelawfirm.com
Martin Ramey
North Carolina State Bar No. 33617
Email: mjr@rhinelawfirm.com
1612 Military Cutoff Rd, Suite 300
Wilmington, North Carolina 28403
Tel: (910) 772-9960
Fax: (910) 772-9062